05

ODP-0-827
23 JUN 1980

MEMORANDUM FOR: Chief, Information Systems Security Group, OS

25X1A FROM: [redacted]
Chief, Management Staff, ODP

SUBJECT: Draft Security Requirements for Automated Information Systems Located in Overseas Installations (U)

1. Office of Data Processing personnel have reviewed the draft of security requirements for automated information systems located in overseas installations. We recognize the importance of prescribing policy in this area and we recommend that the following suggestions be incorporated in the next revision. The last paragraph of this memorandum contains a summary of the recommendations. (U)

2. The requirement for semiconductor volatile memory (IV.D.1.b) may become over-restrictive, e.g., it might affect the use of bubble memories in the future. (S)

3. One of the principal reasons for automating field stations is to make them more efficient and to reduce the vulnerability of information especially if a station is overrun. Although the draft specifies that removable data storage media shall be used (IV.D.1.c), the draft does not address how data should be stored on the media. Considering the possibility of large information banks in the field, stronger guidelines are needed as to what and how much data should be kept in the field and under what conditions. (S)

For instance, should the data stored on field media be encrypted? (S)

If a cassette or a floppy disk were compromised, the problem of damage assessment is not addressed. Since there is no requirement for maintaining volume data set catalogs, the Agency would not know what data were lost. (S)

Perhaps the removability of storage media ought not be an absolute requirement for overseas computers in-as-much-as technology appears to be moving in the direction of non-removability. If this restriction is removed, then procedures should be included to govern how non-removable media is to be handled (e.g., guarded, encrypted, destroyed, etc.). (S)

4. The requirement in IV.D.2.4 for system software to handle all interrupts in a known and secure manner implies that only provably secure operating systems would be allowed. Such operating systems are being developed but are not available now. The draft does not address system software certification or waiver procedures. (U)

5. Paragraph IV.D.5.a.2 specifies that "only those terminals designated for the security classification access level being processed shall be logically connected..." The draft could easily specify that terminals not so designated be electrically disconnected by means of a patch panel or other similar arrangement. The specification of "logically" implies that the system software would control access and this is an unnecessary spillage risk. (S)

6. The requirement for each data file to be controlled by a file password and indicators to describe to the system the type of access authorized (IV.D.5.b.1) is unrealistic for the class of machine planned for the field. Since each dataset must reside on removable media and each storage disk, tape, etc., is to be marked, why not specify that only those media marked at the appropriate level be installed on the system. Or, why not require that system access be authenticated by password and that there be mechanisms restricting file access to authorized users? (S)

7. In the following paragraph (IV.D.5.b.2), access to the master data file is limited to the ADP System Security Officer; there should always be a backup for this function. Also, there is a need in some installations for backup of datasets that require automatic linkage to the master data file. The password file should be protected by encryption such that a system dump or system spillage will not compromise this file. (S)

8. We believe that password procedures (IV.D.5.c) should apply to standalone word processing terminals since this class of terminals can read and write the same data sets as other ADP systems, and up to the same classification levels. (U)

9. If the requirement for file passwords is relaxed, then paragraph IV.D.5.c would have to be revised. (U)

10. The requirement for audit trails presented by paragraph IV.D.6 may be beyond the capabilities of existing system software. (U)

11. The section on Data Processing (V.B) regarding abnormal data processing system operation should be rewritten to be more specific and should concentrate on events that have security implications. For instance, a reported spillage to a terminal or printer should be investigated and would be a valid reason to stop the system. A runaway tape or a disk head crash should not cause the system to be stopped. (S)

12. The section on System Maintenance/Modification may not recognize that the Agency does and will probably continue to use contractor personnel for on-site maintenance and field modification of equipment. (U)

13. The certification of the ISSO on the system software modifications in section VII.B.1.b requires technically expert people to be meaningful. Since these experts are in short supply, even in ADP components, this requirement could be a bottleneck in software updates unless it is treated as a paper exercise. (U)

14. The key to emergency procedures, as mentioned before, is in limiting the amount of data stored in the field, not trying to sanitize or destroy it during an emergency. The draft does not specify that the procedures be exercised so that they are proven and field personnel are fully familiar with them. We suggest a requirement that the ADP Systems Security Officer be responsible for having ADP personnel read the procedures. (U)

15. Equipment procurement sterility is not addressed in the draft. Will there be any policy or guidelines regarding equipment that is Agency unique? (S)

16. In summary, the Office of Data Processing recommends: (S)

a. Prescribe method of storage of data on the removable storage media. (Paragraph 3)

b. Prescribe guidelines as to what and how much data should be kept in the field and under what conditions. (Paragraph 3)

c. Consider encrypting data stored on field media. (Paragraph 3)

d. Require volume data set catalogues be maintained. (Paragraph 3)

e. Consider the use of non-removable storage media. (Paragraph 3)

f. Describe systems software certification or waiver procedures. (Paragraph 4)

g. Specify that terminals not designated for the security classification access level being processed be electrically disconnected. (Paragraph 5)

h. Specify that only media marked at the appropriate level be installed on the system in lieu of requiring file passwords and indicators. (Paragraph 6)

i. Require a backup for the ADP System Security Officer. (Paragraph 7)

j. Provide for backup, where needed, of data sets that require automatic linkage to the master data file. (Paragraph 7)

k. Protect the password file from system dumps or system spillage. (Paragraph 7)

l. Employ password procedures for standalone word processing terminals. (Paragraph 8)

m. Revise paragraph IV.B.5.c if file passwords are not used. (Paragraph 9)

n. Revise the section on system operation abnormalities to concentrate on security implications. (Paragraph 11)

o. Recognize that contractor personnel may be employed for on-site maintenance and field modification of equipment. (Paragraph 12)

p. Review the method of certification of system software modification. (Paragraph 13)

q. Require emergency procedures be exercised. (Paragraph 14)

r. Include policy on equipment procurement sterility. (Paragraph 15)

25X1A

[redacted]

SUBJECT: Draft Security Requirements for Automated Information Systems Located in Overseas Installations (U)

cc: DD/A
C/BD
DD/P
C/ED
C/SPD
SO/ODP

Distribution:
Original - Addressee
1 - C/MS/ODP
1 - O/D/ODP
2 - ODP Registry

25X1A O/D/ODP/[redacted]caj/4011 20 June 1980